

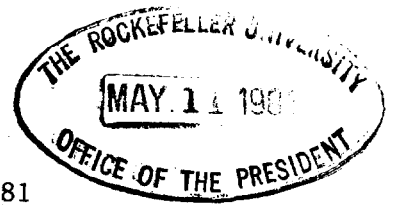
↓

THE MITRE CORPORATION

BEDFORD, MASSACHUSETTS 01730

7 May 1981

D64-181



Dr. Joshua Lederberg
President, The Rockefeller University
1230 York Avenue
New York, New York 10021

Dear Dr. Lederberg:

Bert Fowler passed on to me the ONR report which you sent him citing Prof. Johannesson of the University of Lund and his method of computing logarithms over the finite field of 2^p elements, $GF(2^p)$. This work was formally presented at the IEEE International Symposium on Information Theory (9-12 February 1981) at Santa Monica by his colleague, Dr. Tore Herlestam, of the Swedish Staff of Defense, Department of Signal Security. This "Attempt to Swindle MITRE Corporation" specifically proposed a heuristic algorithm for attacking the public key distribution algorithm I described to you during your visit of 1 April.

The "intriguing" title of the paper, of course, caught our attention, and we were in attendance at the Symposium and had further discussions with Johannesson and Herlestam during their visit to MITRE on 19 February.

The ONR report remains to my knowledge, a basically accurate representation of the current state of this heuristic algorithm. While results for "small" fields of orders 2^{13} , 2^{17} , 2^{31} and 2^{61} have been reported as promising, experiments with larger fields with orders such as 2^{89} , 2^{107} or 2^{127} have been impossible with the computational tools available to the Swedes. For example, while their algorithm computes a logarithm in $GF(2^{31})$ in 7.7 seconds using a 36-bit UNIVAC 1180, extrapolating to $GF(2^{127})$ (assuming a comparable 127-bit computer) results in an expected running time of 29 days. Specialized equipment is therefore recommended.

The more fundamental issue, however, is whether or not we understand the algorithm sufficiently to extrapolate the limited experimental data to larger fields. The current answer is no. As the ONR report makes clear, neither Johannesson nor Herlestam are sure why the algorithm works. In contrast to other published procedures due to Pohlig, Hellman, or Adleman, no sound mathematical theory exists to describe the complexity of this algorithm for increasingly larger fields. Our analysis has been unable to shed any further light on this either, but we have discovered a number of technical shortcomings with the algorithm that may prove fatal as the size of the field grows. Researchers at the University of Southern California and Sandia National Laboratories also concur

4005000

with us in failing to see any inherent theoretical efficiencies in the Swedish algorithm. Until these theoretical questions are answered, or sufficient computational resources are made available to scale larger $GF(2^P)$, a conclusive opinion regarding this work cannot be offered. We plan to continue our analysis of the Johannesson-Herlestan algorithm and hope to make some quantitative comparisons of it with currently accepted methods.

I trust this brief discussion regarding the theoretical security of discrete exponential public key distribution has clarified some of the cryptanalytic issues. I certainly enjoyed our brief discussion regarding the public key concept during your visit, and hope we will be able to resume it at some future date.

Very truly yours,

A handwritten signature in black ink, appearing to read "Brian P. Schanning", with a long, sweeping horizontal stroke extending to the right.

Brian P. Schanning
Principal Investigator
Public Key Data Encryption

BPS/rme

cc: C. A. Fowler